Band 10
Herausgeber: Rüdiger Zarnekow

Stine Labes

Rechtl. Rahmenbedingungen von Cloud Computing

Rechtliche Situation im Öffentlichen Sektor

Technische Universität Berlin
Projektbericht IKM

Projektberichte IKM | 10

Stine Labes

Rechtliche Rahmenbedingungen von Cloud Computing
Rechtliche Situation im Öffentlichen Sektor

Universitätsverlag der TU Berlin

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen National-bibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de/ abrufbar.

Universitätsverlag der TU Berlin 2013
http://www.univerlag.tu-berlin.de

Fasanenstr. 88 (im VOLKSWAGEN-Haus), 10623 Berlin
Tel.: +49 (0)30 314 76131 / Fax: -76133
E-Mail: publikationen@ub.tu-berlin.de

Herausgeber: Prof. Dr. Rüdiger Zarnekow

Satz/Layout: Dr. Koray Erek

Online veröffentlicht auf dem Digitalen Repositorium der Technischen Universität Berlin:
URL http://opus4.kobv.de/opus4-tuberlin/frontdoor/index/index/docId/4131
URN urn:nbn:de:kobv:83-opus4-41312
[http://nbn-resolving.de/urn:nbn:de:kobv:83-opus4-41312]

ISBN 978-3-7983-2627-9 (online)
ISSN 2196-3606 (online)

Projektbeschreibung

Im Projekt „Government Green Cloud Laboratory (Akronym: GGC-Lab)“ werden auf Laborebene die Möglichkeiten des Cloud Computing unter besonderer Beachtung der Energieeffizienz und der Senkung von Energiekosten untersucht. Betrachtet werden typische Anwendungsszenarien der Landes- und Kommunalverwaltungen. Zu diesem Zweck wird erstmalig eine erweiterbare Cloud-Infrastruktur für die öffentliche Verwaltung bundesländerübergreifend durch vier Produktiv-Rechenzentren technisch umgesetzt und erprobt.

Das Projektziel ist die Effizienzsteigerung des IT-Einsatzes in der öffentlichen Verwaltung unter Berücksichtigung der besonderen Betriebs- und Sicherheitsanforderungen. Durch ein dynamisches Lastmanagement sollen die Rechenzentrumseffizienz insgesamt erhöht und damit die Stromkosten gesenkt und klimaschädlichen Effekte verringert werden. Die erforderliche Rechenleistung wird dabei in Abhängigkeit verschiedener (Einfluss-)Parameter (z. B. aktueller Strompreis, aktuelle Gesamteffizienz des Rechenzentrums, verfügbare Kapazitäten) innerhalb der Cloud verteilt. Bei den vier Rechenzentren wird hierfür eine reale Evaluierungsplattform errichtet. Durch die bundesweite Verteilung der Standorte können die Auswirkungen regional und zeitlich unterschiedlicher Stromangebote (Preis, Verfügbarkeit usw.) in die Betrachtung einbezogen werden.

Das Projekt kann durch den hohen Praxisbezug als Best-Practice-Lösung für eine Vielzahl von Anwendungsbereichen dienen und deutlich zur Verbesserung der Umweltbilanz in der IKT beitragen. Die Ergebnisse können z. B. in die Entwicklung einer „Nationalen Government Cloud“, in die Erschließung neuer Geschäftsmodelle, in die Effizienzsteigerung von Weblösungen und in die Integration der Verwaltungs-IT in Energie-Pools einfließen.

Projektteam der TU Berlin

Dipl.-Wirtsch.-Ing. Lars Dittmar
Dipl.-Ing. Stine Labes
Dipl.-Ing. Björn Schödwell
Dipl.-Ing. Marc Wilkens (Teilprojektleiter)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kurzbeschreibung

Die rechtliche Situation und limitierende Rahmenbedingungen sind heute die größte Hürde für die Akzeptanz neuartiger Datenverarbeitung, wie im Cloud Computing. Besonders im Öffentlichen Sektor findet schon heute Datenverkehr und Kommunikation übergreifend über Einrichtungen sowie Städte- und Landesgrenzen hinweg statt. Ob dies künftig auch über Cloud-Dienste abgewickelt werden kann wird in diesem Dokument untersucht.

Mit Fokus auf die Situation im Projekt GGC-Lab, fasst der vorliegende Leitfaden die rechtlichen Themengebiete Vertragsgestaltung sowie Datenschutz und Compliance im Rahmen von Cloud-Diensten zusammen und zeigt Hindernisse auf. Die vertragliche Einordnung von Cloud-Diensten bewirkt unterschiedliche Anforderungen an die Verfügbarkeit des Dienstes sowie Gewährleistung und Haftung bei Verstößen. Für einen Zusammenschluss von öffentlich-rechtlichen IT-Dienstleistern, wie im Projekt GGC-Lab, gelten besondere Bedingungen hinsichtlich des Vergaberechts. Mit Hilfe eines Community-Vertrags werden alle internen Vereinbarungen, Qualitätslevel und Haftungsfragen geklärt. Mit dem Ziel der gemeinsamen Datenverarbeitung von cloudfähigen Fachanwendungen, müssen darüber hinaus spezielle Lizenzverträge mit dem Anbieter der jeweiligen Fachanwendung vereinbart werden. Bei der Verarbeitung personenbezogener Daten mit cloudbasierten Fachanwendung müssen die Forderungen des Datenschutzrechts beachtet werden. Werden durch den Zusammenschluss der IT-Dienstleister wettbewerbsbeeinflussend viele Abnehmer angesprochen, ist die Betrachtung des Kartellrechts eine weitere Hürde, die zu nehmen ist.

Viele Initiativen beschäftigen sich mit diesen komplexen Rechtsfragen und geben Vorschläge wie ihnen zu begegnen ist. Abschließend gibt eine Übersicht über die Inhalte ausführlicher Publikationen Aufschluss über den Stand der gegenwärtigen Diskussionen in diesem Themengebiet.

Schlagwörter: Cloud Computing, rechtliche Rahmenbedingungen, Cloud-Verträge, Datenschutz, Lizenzierung

1 Einleitung

In vorangehenden Teilen dieser Dokumenten-Reihe wurde des Öfteren die Problematik der rechtlichen Unsicherheit bzgl. Cloud Computing angesprochen. Nicht eindeutige und heterogene Rahmenbedingungen in Europa fördern die Unsicherheit. Diese Problematik trifft besonders die Hauptzielgruppe von Cloud-Diensten, die kleinen und mittelständischen Unternehmen (KMU), da diese oft nicht in der Lage sind individuelle und ausführliche rechtliche Prüfungen durchzuführen (Eriksdotter, 2011). Den Öffentlichen Sektor betreffen die rechtlichen Aspekte im Besonderen, da öffentliche Einrichtungen eine größere Verantwortung den Verbrauchern gegenüber tragen. In einer Emnid-Umfrage aus dem Jahr 2011 genießt der Öffentliche Sektor weiterhin das größte Vertrauen in den Datenschutz gegenüber dem Einzelhandel, Banken und Versicherungen, Telekommunikation und Internet Service Providern, Transport und Verkehr sowie, auf dem letzten Platz, Online-Shops (Symantec, 2011).

Das vorliegende Dokument befasst sich mit der Darstellung relevanter rechtlicher Regelungen für die Etablierung einer Cloud-Lösung im öffentlichen Bereich. Ziel dieser Zusammenstellung ist es die rechtlichen Vorgaben aufzuzeigen und die relevanten Reglungen für den Einsatz in Cloud Projekten, besonders im Projekt Government Green Cloud Labor (GGC-Lab), abzuschätzen. Nach dem einleitenden ersten Kapitel erfolgt die Betrachtung der rechtlichen Rahmenbedingungen in Kapitel zwei. Das dritte Kapitel schließt mit einem Fazit zu diesem Thema.

2 Rechtliche Rahmenbedingungen im Öffentlichen Sektor

Die Wahrung der Sicherheit besonders im öffentlichen Bereich, ist juristisch gesehen ein kontroverses Thema. Fehlende rechtliche Regelungen für die neuen Nutzungsformen, wie dem Cloud Computing, ergeben ein Konflikt- und Risikopotential für eine Cloud-basierte Verarbeitung von Informationen. Auch im öffentlichen Bereich werden Daten erhoben, bearbeitet oder weitergeleitet. Dies geschieht zwischen verschiedenen Einrichtungen der Bundesländer sowie zwischen Bundesländern und zwischen Staaten. Eine solche Verarbeitung der Daten in der Cloud unterliegt gewissen Vorgaben, welche nicht alle von der aktuellen Gesetzgebung gedeckt werden können. Als Ansatz diese Lücke zu schließen hat das Bundesministerium für Sicherheit in der Informationstechnologie (BSI)

ein Eckpunkte-Papier zusammengestellt, welches sicherheitsbezogene Mindestanforderungen an einen Cloud-Anbieter beschreibt. Die aufgenommen Eckpunkte beziehen sich auf folgende Themen (BSI, 2010):

1. Sicherheitsmanagement beim Anbieter
2. Sicherheitsarchitektur
3. ID- und Rechtemanagement
4. Kontrollmöglichkeiten für Nutzer
5. Monitoring und Security-Incident Management
6. Notfallmanagement
7. Portabilität und Interoperabilität
8. Sicherheitsprüfung und -nachweis
9. Anforderungen an das Personal
10. Vertragsgestaltung
11. Datenschutz und Compliance

Durch die genannten Kriterien werden Rahmenbedingungen für den Einsatz von Cloud Diensten aufgespannt. Die Anforderungen mit einer rechtlichen Orientierung sind die beiden Punkte „10. Vertragsgestaltung“ sowie „11. Datenschutz und Compliance“. Diese Aspekte werden in den nachfolgenden Abschnitten vertieft.

2.1. Vertragsgestaltung

Verträge enthalten konkrete Vereinbarungen für die zu erbringenden Leistungen sowie die Ansprüche beider Vertragspartner (Anbieter und Abnehmer). Die Leistungsbeschreibung von IT-Diensten wird in der Regel durch Service Level Agreements (SLAs) formuliert. Hier werden die Anforderungen an den Service möglichst genau dargestellt. Die Art der vereinbarten Leistung definiert den anzuwendenden Vertragstyp und die entsprechenden Konsequenzen, z.B. bei der Gewährleistung. Die BITKOM widmet diesem wichtigen Aspekt in einem Leitfaden ein ganzes Kapitel (BITKOM, 2010) und der Verband Eurocloud hat dazu ebenfalls einen Leitfaden veröffentlicht (Eckhardt, et al., 2010). Die wichtigsten Punkte werden hier zusammenfassend erläutert.

2.1.1. Vertragsbeziehungen

Bei der Auswahl eines geeigneten Vertragspartners können ein oder mehrere Anbieter in Frage kommen. Die höchste Transparenz für den Kunden ist gegeben, wenn alles aus einer Hand bezogen wird und Subunternehmer keine Rolle spielen. Auch die Komplexität unterschiedlicher Problemfelder, wie Datenschutz oder Compliance wird dadurch reduziert. Werden seitens des Anbieters weitere Subunternehmer in die Wertschöpfungskette einbezogen, muss der Kunde darauf achten, dass die vertraglichen Verpflichtungen konsistent an die Subunternehmer weitergegeben und erfüllt werden. Folgende Vertragsbeziehungen können im Cloud Computing auftreten (siehe Abbildung 1, in Anlehnung an (BITKOM, 2010)):

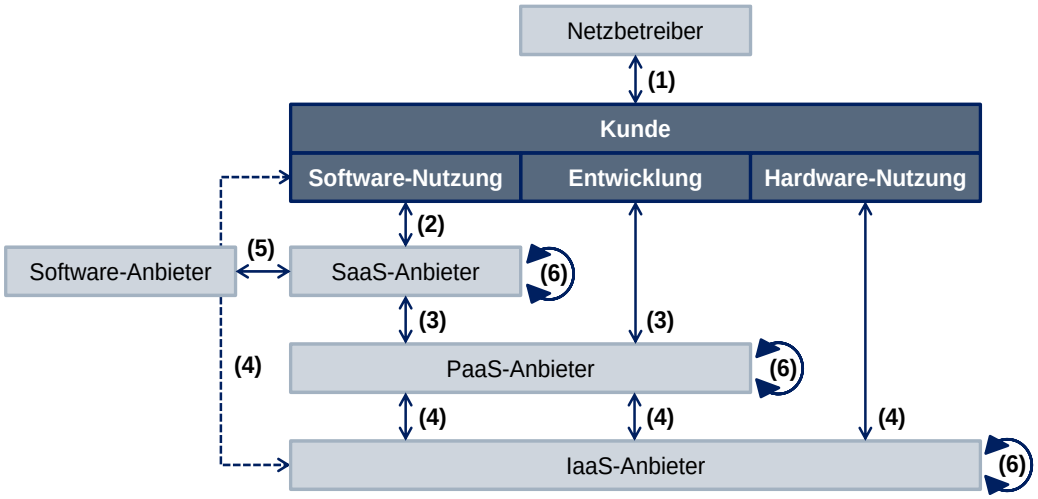

Abbildung 1: Mögliche Vertragsbeziehungen im Cloud Computing

(1) **Netzbetreiber**: Der Vertrag zu einem Bereitsteller des Internetzugangs ist unabhängig von einem Cloud-Anbieter, entsprechend müssen Leistungsanforderungen (z.B. zur Verfügbarkeit) an den Internetzugang getrennt von dem Cloud-Dienst betrachtet werden. Auf diese Vertragsart wird daher im Folgenden nicht weiter eingegangen.

(2) **SaaS-Anbieter**: In dem Verhältnis zum Software-as-a-Service(SaaS)-Anbieter müssen die Leistungsanforderungen (z.B. bzgl. der Vertraulichkeit) an bestehende Subunternehmer weitergeleitet werden. Selten hat der Kunde hier einen direkten Kontakt und Einfluss, so entwickelt sich ein gewisser Unsicherheitsfaktor.

(3) **PaaS-Anbieter**: Als Vertragspartner mit dem Platform-as-a-Service(PaaS)-Anbieter kann sowohl ein Kunde als auch ein SaaS-Anbieter

interagieren, um Softwareentwicklung oder -betrieb auszulagern. Entsprechend wird hier die plattformspezifische Nutzung der Laufzeitumgebung im Betrieb oder die Nutzung der Plattform als Entwicklungsumgebung vereinbart. Anforderungen an die Infrastruktur müssen vom PaaS-Anbieter entsprechend durchgereicht werden.

(4) **IaaS-Anbieter**: Verträge mit Infrastructure-as-a-Service(IaaS)-Anbietern können von PaaS-Anbietern geführt oder direkt mit dem Kunden vereinbart werden, um den Zugang und die Nutzung der Infrastruktur zu regeln. Kunden nutzen die Infrastruktur z.B. zur Kapazitätserweiterung des eigenen Rechenzentrums oder als Subunternehmer über den Pfad eines SaaS- bzw. PaaS-Anbieters. Anforderungen des Kunden werden direkt mit dem IaaS-Anbieter vereinbart, indirekt über den PaaS-Anbieter durchgereicht oder bei Bedarf zusätzlich zu einem SaaS-Vertrag formuliert, wenn eine Sicherung der Anforderungen nicht anders möglich ist.

(5) **Software-Anbieter**: Ist der SaaS-Anbieter nicht gleichzeitig Inhaber der Software, wird hier ein Überlassungsvertrag benötigt. Für typische Cloud-Dienste muss dieser Vertrag beinhalten, dass die Software auf beliebig vielen Servern installiert und von einer unbegrenzten Anzahl von Anwendern genutzt werden darf. Aus SaaS-Anbietersicht spielt die Lizenzierung von Software eine entscheidende Rolle und wird in den nachfolgenden Abschnitten vertieft.

(6) **Community**: Da sich bei einer gemeinsamen Leistungserstellung mehrere IT-Dienstleister zusammenschließen können, muss hier ein weiterer Vertragstyp betrachtet werden. Das Verhältnis der IT-Anbieter zueinander wird durch eine interne Vertragsgestaltung geregelt. Aus diesem Vertrag konstituiert sich die Community der IT-Dienstleister. Intern werden durch diesen Vertrag die gegenseitigen Verpflichtungen und Regeln, sowie die Verteilung der Erlöse festgehalten.

Das GGC-Lab stellt sich gegenüber den Anwendern als Anbieter von Fachanwendungen als SaaS dar. Da die Rechenzentren, auf denen das Projekt basiert, ihre eigenen Plattform- und Infrastruktur-Ressourcen beherbergen, ist hier nur die Betrachtung der Verträge zum Kunden relevant, sowie zu den Anbietern der Software, welche „cloudfähig“ gemacht und als SaaS angeboten werden. Teilweise werden diese Software-Anwendungen hausintern entwickelt, dann ist ein zusätzlicher Vertrag meist hinfällig. Von großer Bedeutung ist für den Verbund

mehrerer Rechenzentren, wie im GGC-Lab, der Community Vertrag. Dieser wird in den nachfolgenden Abschnitten näher betrachtet.

2.1.2. Cloud-Dienst-Verträge

Dieser Abschnitt behandelt die Vertragsbeziehung (2) bis (4) und erläutert die Zuordnung zu bereits definierten Vertragsarten sowie die daraus resultierenden Gewährleistungsrechte des Auftraggebers, bzw. Kunden.

Vertragseinordnung. Das umfangreiche Spektrum und die große Breite der möglichen Cloud-Dienste machen eine pauschale Zuordnung zu einem gesetzlich definierten Vertragstypen nicht direkt möglich. Die für das Cloud Computing typischen Ausprägungen (SaaS, PaaS und IaaS) werden unterschiedlich betrachtet und rechtlich bewertet (siehe Tabelle 1, Vgl. (BITKOM, 2010)).

Tabelle 1: Vertragstypologische Einordnung

Ebene	Vertragstypologische Einordnung
SaaS	SaaS stellt aus rechtlicher Sicht, als zeitlich begrenzter Zugriff auf bereitgestellte Software, eine Art des Application Service Providing (ASP) dar. Nach der Rechtsprechung des Bundesgerichtshofs zu ASP wird daher auch bei SaaS häufig eine mietvertragliche Gestaltung vorliegen. Ergänzend vereinbarte Überwachungs- und Betriebsleistungen haben üblicherweise dienstvertraglichen Charakter.
PaaS	Der für PaaS typische, zeitlich begrenzte Zugriff auf eine bereitgestellte Laufzeit- oder Entwicklungsumgebung entspricht häufig ebenfalls dem Wesen eines Mietvertrags. Ergänzend vereinbarte Überwachungs- und Betriebsleistungen haben üblicherweise dienstvertraglichen Charakter.
IaaS	Im Rahmen von IaaS gilt es zu unterscheiden: ▪ Die reine Bereitstellung einer Hardware-Umgebung und/oder von Speicherplatz erfolgt regelmäßig auf Basis eines Mietvertrags. ▪ Ergänzende Überwachungs- und Betriebsleistungen haben üblicherweise dienstvertraglichen Charakter. ▪ Bestimmte Vertragsgestaltungen, etwa beim Webhosting, können nach Auffassung des Bundesgerichtshofs werkvertraglichen Charakter haben. Dort liegt der Schwerpunkt üblicherweise auf der permanenten Abrufbarkeit der Website und damit einem rechtsgeschäftlichen Erfolg, nicht nur in der Bereitstellung von Webspace.

Laut Leitfäden der BITKOM (BITKOM, 2010) und einem BGH-Urteil aus dem Jahr 2006 (BGH, Az. XII ZR 120/04, 2006) zu dem rechtlich vergleichbaren Application Service Providing (ASP) werden die meisten privatwirtschaftlichen Cloud Computing Leistungen auf mietvertraglicher Basis erfolgen. Für diesen Fall schuldet der Anbieter allerdings eine 100 % Verfügbarkeit des Dienstes, dies erfordert eine sinnvolle vertragliche Regelung. Das Angebot von Fachanwendungen als SaaS im GGC-Lab entspricht einer Einordnung als Mietvertrag. Alle Rechte und Pflichten eines mietvertraglichen Verhältnisses kommen entsprechend zur Anwendung. Zusätzliche Dienste, wie ein User Help Desk, Support, Wartung, Datenspeicherung oder Archivierung haben eher einen Werk- oder Dienstvertrag als Grundlage. Cloud-Dienste erfordern daher einen gemischt-typischen Vertrag.

Gewährleistungsrechte. Wird von zwei Parteien ein geschäftliches Verhältnis eingegangen, bestehen unterschiedliche Ansprüche des Auftraggebers bezüglich Garantie bzw. Haftung und Schadensersatz. Sollten in einem Vertragsverhältnis Leistungsstörungen auftreten, können je nach vertraglicher Ausgestaltung folgende Gewährleistungsrechte bestehen (siehe Abbildung 2, in Anlehnung an (BITKOM, 2010)):

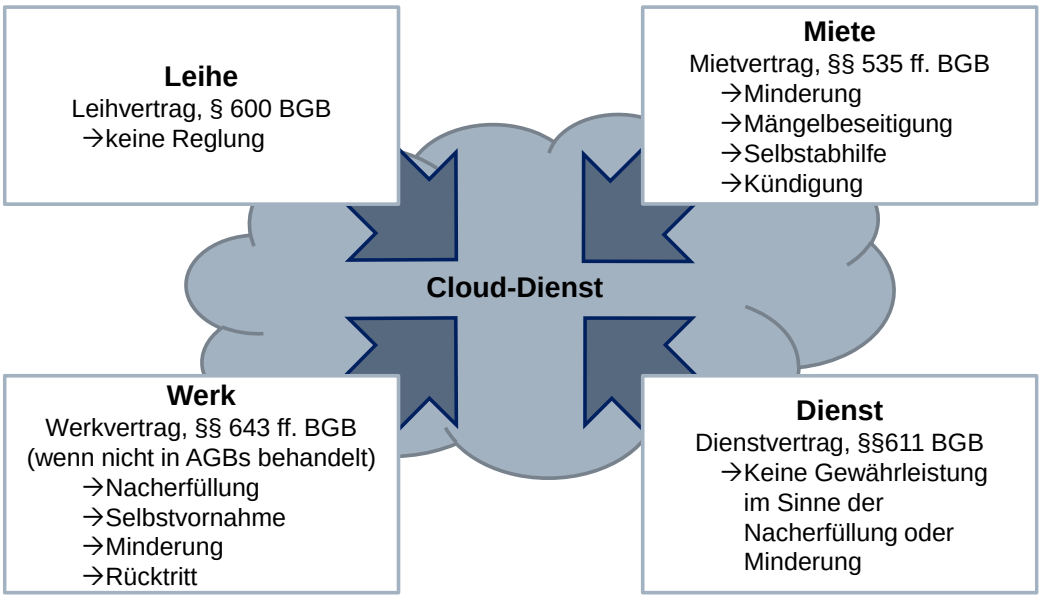

Abbildung 2: Gewährleistung und Haftung

Der **Mietvertrag** besitzt in seiner Auslegung spezifische gesetzliche Gewährleistungsvorschriften. Diese spezifischen Vorschriften sehen eine Minderung bei der

Vergütung vor, sobald Mängel auftreten, die eine Nutzung der Leistung durch den Auftraggeber beeinträchtigen. Eine Behebung der Mängel durch den Auftraggeber ist durch das Prinzip des Cloud Computing nicht möglich, denn Schäden, die durch mangelnde Verfügbarkeit der Cloud Ressourcen oder durch Datenverluste (inklusiver ihrer Sicherungen) sind irreparabel.

Der **Dienstvertrag** definiert keine konkreten Erfolge und findet i.d.R. im Bereich der Beratung Verwendung. Kommt es zu einer Pflichtverletzung des Auftragnehmers (Dienstleisters) so muss der Auftraggeber (Kunde) dieses beweisen. Ein solcher Rechtsstreit sprengt in der Regel die Dauer von einem Monat. Nach einer solchen Dauer kann der Bedarf an den zum damaligen Zeitpunkt benötigten Ressourcen verflogen sein. Eine Entschädigung ist in diesem Fall nur finanziell möglich.

Der **Werkvertrag** beschreibt einen Vertrag zwischen Auftraggeber und Auftragnehmer, bei dem, üblicherweise im Vorfeld, die definierte Leistung vereinbart wird. Werden nicht alle Leistungen im Vertrag festgehalten bzw. spezifiziert ist der Auftragnehmer verpflichtet den geforderten Verwendungszweck „nach mittlerer Art und Güte“ zu erbringen. Gesetzlich wird vorgesehen, dass der Auftraggeber bei einer nicht ordnungsmäßigen Erfüllung ein Recht auf Nacherfüllung durch Nachbesserung oder Neulieferung besitzt. Im Cloud Computing entfällt dem Auftraggeber das Recht zur Selbstvornahme einer Mängelbeseitigung, da dieser keinen Zugriff auf das System durch den Auftragnehmer erhält. Bei Fehlschlag der Nacherfüllung kann der Auftraggeber unter besonderen Bedingungen vom Vertrag zurücktreten.

Der **Leihvertrag** kommt zustande, wenn eine kostenfreie Bereitstellung von Hard- und/oder Software angeboten werden. Für ein solches Angebot bestehen die üblichen gesetzlichen Vorschriften für Leihverträge. Bei einem Leihvertrag haftet der Anbieter nur für grobe Fahrlässigkeit und Vorsatz sowie für arglistiges Verschweigen eines Mangels. Der Auftragnehmer hat durch die unentgeltliche Bereitstellung keine Ansprüche auf Beseitigung von Mängeln oder eine Reduzierung von Vergütung.

Nach außen haftet die Organisation, die den Auftrag erhalten hat. Innerhalb einer Community muss die Haftung dann im Innenverhältnis weitergegeben werden. Der exakte Übergang des Haftungsrisikos muss innerhalb eines Community-Vertrags geregelt werden. Darüber hinaus muss festgelegt werden was passiert, wenn ein Mitglied eine bestimmt Verpflichtung temporär nicht einhalten kann. Die

anderen Mitglieder sollten entsprechend formuliert werden, damit die Last umverteilt werden kann. Eventuelle Strafzahlungen sollten gemäß der Auffassung einer Rechtsexpertin direkt im Gewinnverteilungsschlüssel umgesetzt werden.

2.1.3. Lizenzverträge

Dieser Abschnitt bezieht sich auf die Vertragsbeziehung (5), eines SaaS-Anbieters zu dem Software-Anbieter dessen Software der SaaS-Anbieter in der Cloud anbietet. Dabei muss der Lizenzierungsbedarf der Software näher betrachtet werden.

Software ist gemäß § § 69a ff. UrhG urheberrechtlich geschützt. Gegenstand dieses Schutzes ist der konkrete Quellcode der Software. § 69c UrhG definiert folgende Nutzungsarten von Software, für die eine entsprechende Einräumung eines Rechts mittels einer Lizenz notwendig ist:

- Vervielfältigung
- Umarbeitung
- Verbreitung
- Öffentliche Wiedergabe (einschl. der öffentlichen Zugänglichmachung)

Diese Liste ist nicht abschließend, weitere technisch und wirtschaftlich eigenständige sowie klar abgrenzbare Nutzungsarten sind urheberrechtlich anzuerkennen und entsprechend schutzwürdig. Wird Software von einem Anbieter für die Bereitstellung an Kunden in der Cloud verwendet (SaaS), besteht die Frage nach der dabei urheberrechtlich relevanten Nutzungshandlung.

Eine **Vervielfältigung** (§ 69c Nr. 1 UrhG) einer Software besteht, wenn ein Programm installiert oder zur Bearbeitung in den Arbeitsspeicher geladen wird. Der Aufruf der Software wird zwar durch den Kunden ausgelöst, findet bei einer Cloud-Anwendung jedoch nur auf dem System und unter der Steuerungshoheit des Anbieters statt. Die Software wird vom Anbieter gehostet und betrieben, daher muss sich dieser vom Software-Anbieter (sofern er das nicht selbst ist) ein Recht zur Vervielfältigung einräumen lassen. Cloud-Software ist in der Regel mandantenfähig und kann mehrere Mandanten bedienen, ohne dass für jeden Kunden eine getrennte Software-Instanz benötigt wird. Daher ist für das Betreiben von Cloud-Software rein rechtlich nur eine Lizenz erforderlich (Trusted Cloud, 2012). Bei nicht mandantenfähiger Software, die z.B. auf Grundlage eines IaaS für jeden Kunden getrennt zur Verfügung gestellt wird, ist entsprechend für jeden Kunden ein Vervielfältigungsrecht notwendig. Sobald der Kunde auch auf

seinem System eine Installation vornehmen muss, wird auch hier ein Vervielfältigungsrecht erforderlich. Dies ist bei einer Cloud-Software (rein definitorisch) nicht der Fall, trifft jedoch auf den Client (meist Internet-Browser oder Apps) zu, mit welchem der Kunde auf die Software zugreift. Der Gegenstand der Vervielfältigung ist bei dem Kunden also nicht die Cloud-Software, sondern der Client, welcher meist eine Standardsoftware und beim Kunden bereits lokal installiert ist. Ist dies nicht der Fall und der Kunde greift über einen proprietären und von dem SaaS getrennt zu installierenden Client (z.B. App) auf die Software zu, bedarf es einer zusätzlichen Einräumung des Vervielfältigungsrechts durch den Anbieter.

Wird eine **Umarbeitung** der Software durch den Anbieter vorgenommen, um sie cloudfähig zu machen und als SaaS bereitzustellen, ist dafür eine entsprechende Lizenz notwendig (Vgl. § 69c Nr. 2 UrhG). Davon unberührt sind Änderungen zur Fehlerbeseitigung (§ 69d UrhG) oder die Erstellung von Schnittstellen (§ 69e UrhG) zur Förderung der Interoperabilität. Im Projekt GGC wird eine Standard-Software cloudfähig gemacht und damit weitgehend verändert, was das Erfordernis einer Rechteinräumung für die Umarbeitung nach sich zieht.

Eine **Verbreitung** der Software im Sinne des § 69c Nr. 3 UrhG ist fraglich, da der Kunde beim Mieten der Cloud Software kein zeitlich begrenztes Recht auf Installation und Betrieb der Software erwirbt. Das würde ggfs. nur auf die beim Kunden installierte Client Software zutreffen.

Bezüglich der **Wiedergabe** der Software ist die Bereitstellung an Kunden vergleichbar mit einer **öffentlichen Zugänglichmac**hung (Vgl. § 69c Nr. 4 UrhG). Gemäß § 15 Abs. 3 UrhG bezieht sich das „öffentlich“ auf eine Mehrzahl nicht miteinander bekannter Personen und würde damit sogar auf die Belegschaft eines Unternehmens zutreffen, denen die Software nur in einer Private Cloud angeboten wird. Damit handelt es sich bei der Zugänglichmachung von Software in einer Cloud um einen öffentlichen Vorgang. Als weitere Voraussetzung trifft die Wahlfreiheit des Zugangs bzgl. Ort und Zeit zu, denn sie ist eine ausdrückliche Eigenschaft von Cloud-Diensten. Die Zugänglichmachung wird kontrovers diskutiert, denn es wird nicht der Quellcode der Software, sondern nur die Weboberfläche zugänglich gemacht. Da mittels der Weboberfläche jedoch auf die Funktionalität der Software zugegriffen werden kann, hat sich ein Konsens gebildet, wonach damit eine Zugänglichmachung der Software vorliegt (Trusted Cloud, 2012). Nach einer anderen Auffassung besteht bei der Bereitstellung der Funktionalität von SaaS ein Nutzungsrecht eigener Art (sui generis). In diesem Fall

muss sich der Anbieter einer Software konkrete Rechte durch den Hersteller der Software einräumen lassen (Trusted Cloud, 2012). Die Spezifizierung dieser Rechte durch den Anbieter gegenüber dem Software-Hersteller verschärft die Anforderungen an die Vertragsgestaltung und ließe sich durch die Annahme der öffentlichen Zugänglichmachung vermeiden. Bis zur höchstrichterlichen Klärung des Sachverhalts sollte in den Lizenzverträgen ausdrücklich klargestellt werden, dass die Software zur Bereitstellung in einer Cloud genutzt werden darf.

Zusammenfassend zeigt die nachfolgende Grafik auf welcher Seite, bezogen auf Anbieter und Anwender, welche Rechte an welcher Software benötigt werden (siehe Abbildung 3). Im GGC-Lab wird eine Fachanwendung von einem Software-Anbieter cloudfähig gemacht und als SaaS angeboten. Für den SaaS-Anbieter (das GGC-Lab) gelten also alle Anforderungen an die benötigten Lizenzrechte bzgl. des Anwendungsprogramms (Fachanwendung vom entsprechenden Software-Anbieter), ein zusätzlicher proprietärer Client wird nicht verwendet. Festzuhalten ist, dass durch die Umarbeitung zu einem mandantenfähigen Cloud-Dienst theoretisch nur eine einzige Vervielfältigungslizenz vom Software-Anbieter einzuholen ist und mit der dann cloudfähigen Anwendung mehrere Anwender bedient werden können.

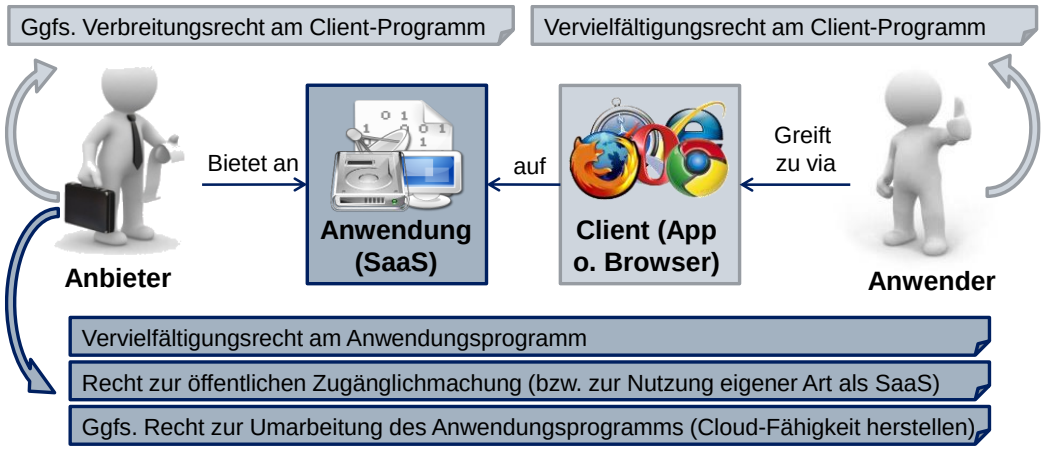

Abbildung 3: Lizenzierungsbedarf bei SaaS

Die Beschaffung der Lizenzen für die Fachanwendungen sollte laut der Aussage einer Rechtsexpertin von der Community vorgenommen werden, nicht durch die einzelnen Mitglieder. Im Öffentlichen Sektor orientiert sich der Anwendungsbereich der Lizenz oft am Umfang der zu verarbeitenden Daten, welcher z.B. eine

Umlage auf die zu verwaltenden Bürger darstellt. Wenn eine Lizenz für die gesamte Community beschafft wird, so muss als Umlageschlüssel hier die Gesamtanzahl potentieller Bürger betrachtet werden. Die Berechnungsgrundlage für die Lizenz einer Community wäre damit unverhältnismäßig größer als die der einzelnen Anbieter, da die Anwendung möglicherweise nicht jedes Community Mitglied für ihre Bürger anzuwenden gedenkt. Wird die Lizenz weiterhin einzeln beschafft, muss diese flexibel verschiebbar sein, damit Daten in einem anderen Rechenzentrum verarbeitet werden können. Durch den höheren Umlageschlüssel oder die gehobene Flexibilität bei einer gemeinsamen Leistungserstellung können die Lizenzkosten daher enorm sein. Darüber hinaus ist laut der Rechtsexpertin bei einer Verschiebung personenbezogener Daten unbedingt eine Vermischung der Daten mit denen des verarbeitenden Rechenzentrums zu vermeiden.

2.1.4. Community-Vertrag

Die Vertragsbeziehung (6), der Community-Vertrag, ist die Grundlage für eine gemeinschaftliche Leistungserbringung, wie sie beispielsweise im GGC-Lab umgesetzt wird. Als Rechtsformen für die Community Cloud kommen sowohl eine Genossenschaft als auch ein Zweckverband in Frage.

Das Wesen der Genossenschaft wird im § 1 Abs. 1 GenG wie folgt beschrieben: „Gesellschaften von nicht geschlossener Mitgliederzahl, deren Zweck darauf gerichtet ist, den Erwerb oder die Wirtschaft ihrer Mitglieder oder deren soziale oder kulturelle Belange durch gemeinschaftlichen Geschäftsbetrieb zu fördern (Genossenschaften), erwerben die Rechte einer "eingetragenen Genossenschaft" nach Maßgabe dieses Gesetzes“. Diese Genossenschaft, z.B. einer öffentlich-rechtlichen Körperschaft, wird vertraglich in einer schriftlichen Satzung festgehalten (§ 5 GenG). Eine Genossenschaft muss aus mindesten drei Mitgliedern bestehen (§ 4 GenG), einen Vorstand besitzen sowie bei mehr als 20 Mitgliedern einen Aufsichtsrat bestimmen (§ 9 Abs. 1 GenG). Der Vorstand hat dafür zu sorgen, dass die Buchführungspflicht (§ 33 Abs. 1 GenG) ordnungsgemäß ausgeübt wird. Die meisten Änderungen der Satzung müssen mit einer dreiviertel Mehrheit abgesegnet werden (§ 16 GenG), der Beitritt (§ 15 GenG) und die Kündigung (§ 65 GenG) können dagegen relativ einfach abgewickelt werden. Das Rechtsverhältnis zwischen Genossenschaft und Mitgliedern richtet sich nach den Bestimmungen der Satzung (§ 18 GenG).

Die rechtliche Grundlage für Zweckverbände bilden Gesetze über die kommunale Gemeinschaftsarbeit (GKG) der jeweiligen Bundesländer. Institutionen können sich mit einem öffentlich-rechtlichen Vertrag zu einem Zweckverband zur gemeinsamen Erledigung einer bestimmten öffentlichen Aufgabe zusammenschließen (§ 4 Abs. 1 GKG). Als Mitglieder können in einem Zweckverband auch Personen des Privatrechts aufgenommen werden, solange die Erfüllung der Verbandsaufgaben dadurch gefördert wird (§ 4 Abs. 3 GKG). Auch diese Körperschaft verlangt eine Satzung (§ 7 GKG), in welcher die Mitglieder, die Aufgaben und die Finanzierung festgelegt werden (§ 9 GKG). Organe des Zweckverbandes sind die Verbandsversammlung und der Verbandsvorsteher (§ 14 GKG). Änderungen der Verbandssatzung sowie Neuaufnahmen oder Ausscheiden von Mitgliedern bedürfen einer Abstimmungsmehrheit von zwei Dritteln der satzungsmäßigen Stimmenzahl (§ 20 Abs. 1 GKG).

Beide Varianten bieten Vor- und Nachteile. Wie eine konkrete Gestaltung im entsprechenden Einzelfall aussieht ist eine komplexe Auseinandersetzung mit der betreuenden Rechtsabteilung. Die gewählte Rechtsform sollte in jedem Fall die Inhouse-Fähigkeit nicht beeinträchtigen, diese wird im Kapitel „Compliance“ näher erläutert. Bei einer Genossenschaft setzt das voraus, dass keine privat-rechtlichen Mitglieder aufgenommen werden. Die „Quasi-Anbindung“ notwendiger privat-rechtlicher Partner, z.B. für den Lastverschiebungsalgorithmus oder weiterer externer Software-Lieferanten, wäre möglich, wenn die proprietäre Software als Lizenz erworben wird und deren Pflege rechtskonform ausgeschrieben wird. In diesem Fall wird wohl nur der Hersteller der proprietären Software für deren Pflege angemessen in der Lage sein und damit den Ausschreibungsprozess gewinnen.

2.2. Datenschutz

Unter Datenschutz wird laut § 1 des Bundesdatenschutzgesetzes (BDSG) der Schutz des Persönlichkeitsrechts bei der Verarbeitung personenbezogener Daten verstanden. Personenbezogene Daten unterliegen besonderen rechtlichen Bedingungen (EG Richtlinie 95/46/EG, 1995) (BDSG), die den Anwendungsbereich des Datenschutzrechts öffnen. Herausforderungen durch neue Informationstechnologien sowie die Globalisierung des Datenschutzes erfordern eine Aktualisierung der fast 20 Jahre alten Datenschutzrichtlinie. Im Januar 2012 hat die Europäische Kommission einen Vorschlag für eine neue Datenschutzverordnung vorgestellt, die die bisherige EG-Richtlinie zum Datenschutz (95/46/EG) ablösen

soll. Bislang existiert keine gemeinsame Position im EU Parlament, die Verhandlungen mit den Mitgliedstaaten werden noch lange andauern (Feld, 2013). In der Bundesrepublik Deutschland ist die Zielsetzung des Datenschutzes im § 1 BDSG geregelt. Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (Fraunhofer FOKUS, 2010).

Bei der Nutzung von Cloud-Diensten kommt es zu einer Verarbeitung und Speicherung personenbezogener Daten, die vorwiegend auf nicht lokalisierbaren verteilten Servern des Anbieters liegen. Dabei ist nicht nachvollziehbar, wo die Daten gespeichert und verarbeitet werden, besonders wenn der Anbieter selbst Cloud-Dienste für seine eigene Dienstleistung von Sublieferanten bezieht (Budszus, et al., 2011). Wichtige Aspekte des Datenschutzes für das Cloud Computing werden in den folgenden Unterabschnitten erläutert werden.

2.2.1. Personenbezogene Daten

Hervorzuheben ist, dass sich der Datenschutz nur auf personenbezogene Daten bezieht d.h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person – juristische Personen sind ausgenommen (§ 3 Abs. 1 BDSG).

Abbildung 4 gibt einen Überblick der verschiedenen Kategorien von Daten bei denen ein Schutzbedarf besteht (Vgl. (BITKOM, 2010)). Im GGC-Lab werden in Abhängigkeit von den angebotenen Fachanwendungen als Cloud-Dienst auch personenbezogene Daten verarbeitet. Die grundsätzlichen Regelungen des Datenschutzrechts werden nachfolgend betrachtet und die Datenschutz-Anforderungen in eine Cloud-Umgebung transferiert.

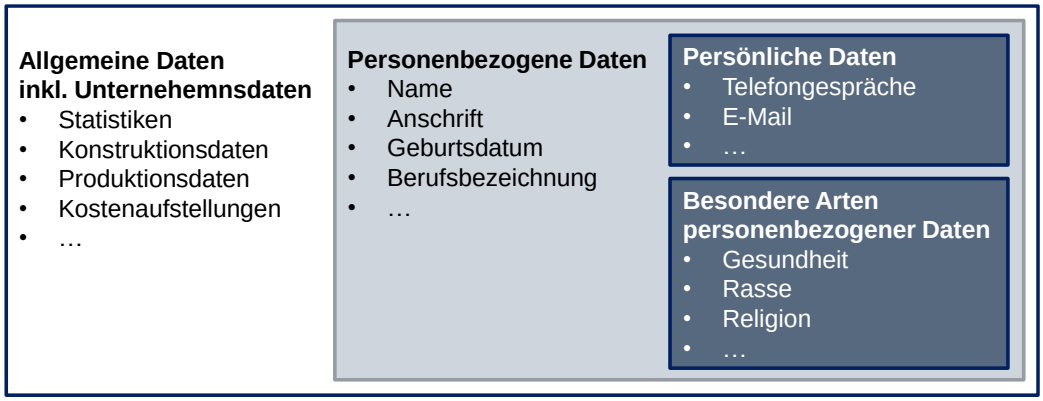

Abbildung 4: Kategorien personenbezogener Daten

2.2.2. Grundprinzipien des Datenschutzrechts

Es existieren vier Grundprinzipien des Datenschutzrechts, welche als Basis für die Schutzziele der Betroffenen dienen:

- „**Verbot mit Erlaubnisvorbehalt** (§ 4 Abs. 1 BDSG): Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind grundsätzlich verboten, es sei denn, es liegt eine Einwilligung des Betroffenen oder eine entsprechende Zulässigkeitsnorm vor.
- **Grundsatz der Zweckbindung** (§ 4 Abs. 3 Nr. 2, § 28 Abs. 1 S. 2, Abs. 2 BDSG): Personenbezogene Daten des Betroffenen dürfen nur zu dem Zweck verarbeitet oder genutzt werden, zu dem sie auch erhoben wurden. Gibt es im Einzelfall mehrere Zwecke, so sind diese auch im Vorfeld eindeutig zu benennen (aktuelles Beispiel: Steuer-Identifikationsnummer darf ausschließlich für steuerliche Zwecke genutzt werden).
- **Grundsatz der Transparenz** (§§ 4 Abs. 3, 33 BDSG) **und Einwilligung** (§ 4a BDSG): Durch das Transparenzgebot soll der Betroffene beurteilen können, ob er seine Daten preisgeben möchte oder nicht. Hierzu benötigt er folgende Mindestangaben: Identität der verantwortlichen Stelle und Zweck der Erhebung.
- **Grundsatz der Datenvermeidung und Datensparsamkeit** (§ 3a BDSG): Das Ziel im Rahmen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten besteht grundsätzlich darin, so wenig personenbezogene Daten wie möglich zu verarbeiten (In der Versicherungsbranche dürfen z.B. ausschließlich die zur Beurkundung eines Risikos erforderlichen Daten erhoben, verarbeitet und genutzt werden). Darüber hinaus sind informationstechnische Systeme so zu konzipieren, dass sie mit so wenig personenbezogenen Daten wie möglich arbeiten. Ferner besteht das Ziel dieses Grundsatzes darin, – sofern sinnvoll nutzbar – Daten zu anonymisieren oder zumindest zu pseudonymisieren.“ (Duisberg, et al., 2011)

Ein Eckpunkte-Papier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahr 2010 betont bei den Datenschutz-Grundsätzen darüber hinaus das Verbot der Profilbildung. Hier soll mit einer gesetzlichen De-

finition der Profilbildung die Zusammenführung und Verknüpfung von personenbezogenen Daten zu Profilen ohne Einwilligung des Betroffenen verhindert werden (BfDI, 2010).

Mithilfe dieser Regelungen soll den Betroffenen die Möglichkeit der Transparenz gegeben werden und es ihnen so ermöglichen die genannten Grundsätze einzufordern. Hervorgehoben wird dies durch den Auskunftsanspruch des Betroffenen nach § 34 BDSG.

2.2.3. Schutzziele des Datenschutzrechts

Die Schutzziele des Datenschutzrechts definieren sich dadurch, dass sie dem Betroffenen jegliche Entscheidungs- und Kontrollgewalt zuschreiben, über die Erhebung und Verwendung von Informationen seiner Person. In bestimmten Fällen, in denen aufgrund anerkennenswerter überwiegender Interessen eines Dritten die Befolgung der Schutzziele nicht mehr interessengerecht wäre, können diese eingeschränkt werden. Zur Veranschaulichung können die Daten eines Betroffenen z.B. nicht gelöscht werden, solange der Dateninhaber diese benötigt, um einen Vertrag durchzuführen, um sich gegen Ansprüche des Betroffenen zu verteidigen oder diese aus anderen rechtlichen Gründen aufbewahren muss (Duisberg, et al., 2011). Konkret werden die „Rechte des Betroffenen“ im § 6 BDSG geregelt und umfassen folgende Punkte:

- „**Auskunft** über die zu ihrer Person gespeicherten Daten. Dieses Recht schließt ein, dass Auskunft über die Herkunft, die Empfänger, an die die personenbezogenen Daten weitergegeben wurden, und den Zweck der Speicherung erlangt werden kann.
- **Berichtigung**, wenn fehlerhafte Daten gespeichert werden.
- **Sperrung**, soweit die Unrichtigkeit der Daten nachgewiesen werden kann.
- **Löschung**, wenn die Speicherung der Daten unzulässig ist oder die Daten nicht mehr benötigt werden (falls Aufbewahrungsfristen zu beachten sind, eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigen würde oder nur mit unverhältnismäßigem Aufwand durchgeführt werden kann, müssen solche Daten gesperrt werden).
- **Widerspruch** gegen die Datenverarbeitung, sofern die Datenverarbeitung nicht durch eine Rechtsvorschrift vorgeschrieben ist.
- **Schadensersatz** wegen einer unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten.“

2.2.4. Datensicherheit

Datensicherheit, auch als Informationssicherheit bezeichnet, ist ein Zustand von informationsverarbeitenden und -lagernden Systemen und dient der Sicherstellung des Datenschutzes. Sie umfasst die drei folgenden Schutzziele:

- **Vertraulichkeit**: kein unbefugter Informationsgewinn
- **Integrität**: keine unbefugte Modifikation der Daten
- **Verfügbarkeit**: keine unbefugte Beeinträchtigung der Funktionalität des Systems

Zur Erfüllung der Datensicherheit bestehen verschiedene Anforderungen an die Auslagerung von Datenverarbeitung. Das BDSG erfasst in der „Anlage zu § 9“ eine Aufzählung von technisch-organisatorischen Maßnahmen, welche von der verantwortlichen Stelle erfüllt werden müssen. Es sollen dabei folgende Punkte beachtet werden:

- **Zutrittskontrolle**: Unbefugten den physischen Zutritt zu Anlagen der Datenverarbeitung(DV) verwehren.
- **Zugangskontrolle**: Nur berechtigten Personen den logischen Zugang ermöglichen (z.B. durch die Vergabe von Passwörtern).
- **Zugriffskontrolle**: Zugriff nur auf Daten ermöglichen, die für die eigene Rolle erforderlich sind.
- **Weitergabekontrolle**: Gewährleisten, dass Daten beim Transport oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (z.B. Verschlüsselung und sicheres Löschen von Daten).
- **Eingabekontrolle**: Möglichkeit der nachträglichen Überprüfung des Nachweises, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind (z.B. durch geeignete Protokollierung).
- **Auftragskontrolle**: Sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, auch nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.
- **Verfügbarkeitskontrolle**: Schutz vor ungewolltem Verlust oder Zerstörung von Daten (z.B. Absicherung durch Datensicherungen, redundante Systeme und unterbrechungsfreie Stromversorgungen).
- **Trennungskontrolle**: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

Zu beachten ist dabei, dass sich das Schutzniveau immer anhand der zu verarbeitenden Daten bemisst. Werden sensiblere Daten bearbeitet, muss ein erhöhtes Schutzniveau installiert werden.

Bei Datenpannen, im Sinne einer unrechtmäßigen Kenntniserlangung von Daten (§ 42a BDSG), besteht eine aktive Informationspflicht gegenüber den Betroffenen und den zuständigen Aufsichtsbehörden.

2.2.5. Datensicherheit in der Cloud

Bedrohungen der Datensicherheit können beeinflusst werden durch die Öffnung des zu unterhaltenden Cloud-Dienstes zum Internet. In Abhängigkeit zur Öffnung der Cloud zu Netzwerkstrukturen des Internets ergeben sich verschiedene Bereitstellungsmodellen (Armbrust, et al., 2009) (BITKOM, 2009) (Fraunhofer FOKUS, 2010), die bereits im Kapitel A1, Teil 1 der losen Blattsammlung vorgestellt wurden. Diese Bereitstellungsmodelle beschreiben die Nutzung nicht-öffentlicher Netzwerkinfrastrukturen und Mandantentrennung (Private Cloud) über Mischvarianten (Hybrid Cloud) bis zur ausschließlichen Nutzung öffentlicher Netzwerkstrukturen und mandantenfähiger Dienste (Public Cloud). Je offener das Bereitstellungsmodell gehalten wird, desto niedriger ist der Grad der Weisungs- und Direktionsmöglichkeiten bzgl. des Sicherheitsniveaus des Cloud-Dienstes. Im deutschen Datenschutz verlangt der Gesetzgeber daher, dass der Auftraggeber einer Datenverarbeitung mindestens Kenntnis über den physischen Ort der Daten besitzen muss. Dies wiederspricht dem Grundsatz einer Public Cloud, da es aus technischer Sicht keinen Grund zu territorialen Grenzen gibt (Weichert, 2011). Öffentliche Cloud-Dienste erhalten daher eher keine Datenschutzempfehlung (BITKOM, 2010).

Die Sicherstellung des Datenschutzes verhält sich auch auf den verschiedenen Ebenen von Cloud-Diensten unterschiedlich, um Vertraulichkeit, Integrität und Verfügbarkeit abzusichern (Budszus, et al., 2011) (siehe Abbildung 5).

Das GGC-Lab bietet seine Cloud-Dienste in einer Community Cloud an, also einem Verbund mehrerer privater Clouds. Die Verbindung zwischen den jeweiligen privaten Ressourcen und Netzwerken der IT-Dienstleister wird via Virtual Private Networks (VPNs) hergestellt. Durch zusätzliche Verschlüsselungstechniken wird eine sichere Cloud-Basis geschaffen, alle anderen beschriebenen Anforderungen der Ebenen IaaS, PaaS und SaaS greifen zusätzlich.

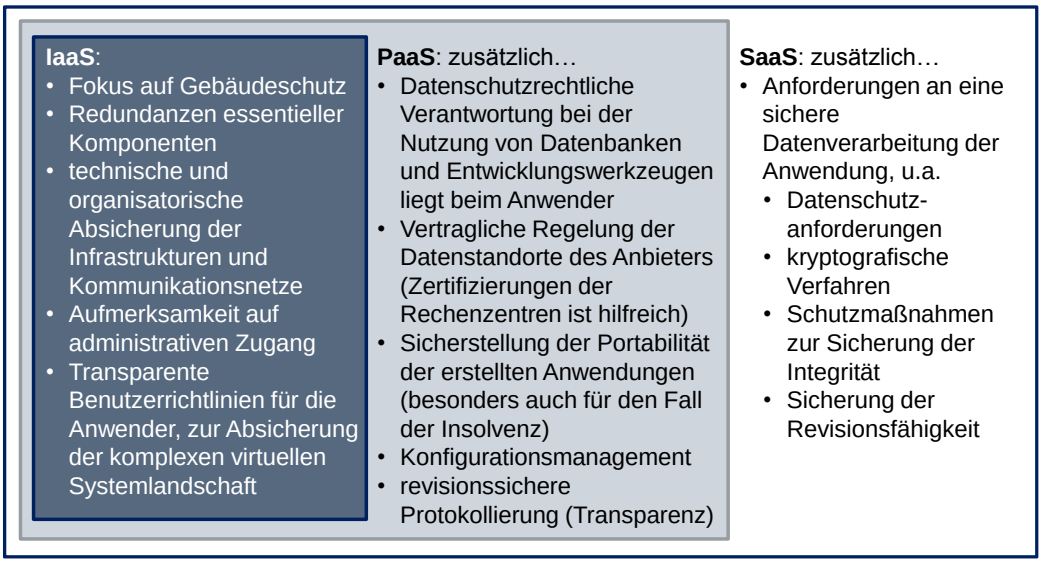

Abbildung 5: Datensicherheit auf den Cloud-Ebenen

2.2.6. Sicherheitsmanagement in der Cloud

Zur Sicherstellung der Anforderungen des Datenschutzes und der Datensicherheit sowie der Vertrauenssteigerung gegenüber den Kunden, empfiehlt es sich besonders als Anbieter von Public Cloud Diensten folgende Aspekte zu beachten (Hofer, 2010):

- **IT-Prozessmodell**: Erstellung eines definierten Vorgehensmodells aller IT-Prozesse (z.B. nach ITIL oder COBIT)
- **Informationssicherheits-Managementsystem**: Implementation eines anerkannten Informationssicherheits-Managementsystem (z.B. nach dem IT-Grundschutzkatalog des BSI oder der ISO 27001)
- **IT-Sicherheitskonzept**: Erstellung und Nachweis (Zertifizierung) eines IT-Sicherheitskonzepts für die Cloud (inkl. 24/7-Support, Notfallmanagement etc.)
- **Mandantentrennung**: Zuverlässige mandantenfähige Gestaltung der Cloud-Plattform
- **Monitoring**: Implementation eines Monitoring-Systems, zur Bereitstellung umfangreicher Daten des Cloud-Dienstes für den Nutzer
- **Regelmäßige Prüfung**: Regelmäßige Prüfung des IT-Sicherheitszustand und transparente Bereitstellung der Prüfnachweise für den Nutzer
- **Vertrauenswürdiges Personal**: Sicherstellung der Vertrauenswürdigkeit und des regelkonformen Handelns des Personals

2.2.7. Deutscher Datenschutz im Ausland

Welches Recht (hier: Datenschutzrecht) greift, wird über das Sitzlandprinzip bestimmt. Dort wo sich die Ressourcen befinden, greift das geltende Recht. Werden bspw. Daten in einem Rechenzentrum in Irland verarbeitet greift das irische Gesetzt zum Datenschutz und damit eventuell ein niedrigeres Datenschutzniveau gegenüber dem deutschen Datenschutz. Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, plädiert auf dem CloudForum 2012 (Berlin) für ein „Ziellandprinzip“. Dies würde das Datenschutzniveau des gezielt angesprochenen Marktes erfordern (nicht das der ganzen Welt, auch wenn der Cloud-Dienst dort theoretisch über das Internet verfügbar ist).

Eine Ausnahme zum Sitzlandprinzip ist gegeben, wenn die personenbezogenen Daten in einer Niederlassung in Deutschland verarbeitet werden (§ 1 Abs. 5 Satz 1 BDSG). Diese Ausnahme greift ebenfalls, wenn sich die verantwortliche Stelle außerhalb des EU/EWR-Raums befindet und personenbezogene Daten in Deutschland erhoben, verarbeitet oder genutzt werden. Bei dieser Variante muss die ausländische Stelle zusätzlich einen sogenannten Inlandsvertreter bestellen (Duisberg, et al., 2011). Durch einen solchen Inlandsvertreter kann nach § 1 Abs. 5 Satz 2 BDSG das deutsche BDSG greifen und die Daten müssen nach dem deutschen Datenschutzgesetz geschützt werden.

Die Einhaltung der deutschen Datenschutzregelungen kann als Wettbewerbsvorteil gegenüber den am internationalen Markt vertretenen Mitbewerbern fungieren. Die betroffenen Bürger, bzw. Kunden, sehen in der Einhaltung, bzw. der Wahrung ihrer personenbezogenen Daten, einen Vertrauensbeweis (Volkmer, 2008). Werden die deutschen Datenschutzbestimmungen umgesetzt, beinhaltet dies nicht nur einen Schutz vor Bußgeldern, Strafen und Haftungsfällen sondern bietet Vorteile für die Bürger und die verantwortlichen Einrichtungen. Es zeigt sich, dass durch die Anwendung des Datenschutzes die Sicherheit und Leistungsfähigkeit einer Einrichtung verbessert und Risiken minimiert werden können (Volkmer, 2008).

2.3. Compliance

Mit Compliance wird die nachweisbare Einhaltung von Regeln und rechtlichen Bestimmungen bezeichnet. Das Ziel der Cloud Compliance ist die Schaffung von Transparenz und Sicherheit für alle Anspruchsgruppen des Cloud-Dienstes

(BITKOM, 2010). Compliance kann durch Zertifikate oder Gütesiegel sichtbar gemacht werden. Neben dem Nachweis der Einhaltung von Datenschutzanforderungen bestehen für den Öffentlichen Sektor spezielle Rechtsgebiete, die in den folgenden Abschnitten erläutert werden.

2.3.1. Organisations- und Vergaberecht

Die Zusammenarbeit von Verwaltungen muss mit dem Organisations- und Vergaberecht vereinbar sein (Rechtsstaatsprinzip Art. 20 GG).

Das Organisationsrecht umfasst das Recht, welches die Schaffung und Führung von organisatorischen Gebilden zum Gegenstand hat. Dieses Recht ist für die Bildung einer Government Cloud in dem Punkt relevant, um eine Organisation zu bilden, die die gewünschte Cloud etabliert. Diese Organisation unterliegt dann in der Regel der jeweiligen Kommune oder öffentlichen Anstalt, ist dabei eigenständig und kann in eigenem Namen handeln. In der Praxis zeigen sich eine Reihe von Anwendungsbeispielen gewählter Organisationsformen, welche im Kapitel A1, Teil 2 „Cloud Computing in der Öffentlichen Verwaltung“ bereits erläutert wurden.

Europäisches Recht bzgl. Zusammenarbeit ist in Deutschland in dem Gesetz gegen Wettbewerbsbeschränkungen (GWB) umgesetzt. Damit es zu einer Zusammenarbeit kommt, müssen nach dem Art. 20 GG sowie dem Vergaberecht Deutschlands und der EU die Aufträge öffentlich in einem Verfahren vergeben werden (§ 97 GWB). Es besteht somit ein Grundsatz zur Ausschreibung für alle Verwaltungen, gleich ob sie öffentlich-rechtlich oder privatrechtlich organisiert sind (§ 98 GWB). Für einen rechtmäßigen Ablauf der Vergabe existiert das Vergaberecht. Das Vergaberecht regelt die Abläufe und Forderungen bei der Vergabe öffentlicher Aufträge. Eine Vergabe kann dazu führen, dass der Auftrag an eine andere Partei erteilt wird, in diesem Fall ist das geplante Vorhaben hinfällig. Um ein solches gemeinsames Vorhaben realisieren zu können, besteht die Möglichkeit den Vergabeprozess unter folgenden Voraussetzungen zu umgehen:

(1) wenn ein gesetzliches Ausschließbarkeitsrecht besteht,
(2) wenn bestimmte Schwellenwerte nicht erreicht werden,
(3) bei erhöhter Sicherheit etc.,
(4) wenn Inhouse-Voraussetzungen vorliegen oder
(5) wenn eine Öffentliche Aufgabe wahrgenommen wird.

Zu (1): Das gesetzliche Ausschließbarkeitsrecht gilt nach § 100 Abs. 2 Lit. g GWB, welcher besagt, dass ein auf ein Gesetz oder eine Verordnung beruhendes ausschließliches Recht zur Erbringung der Leistung besteht. Beispiele für einen solchen Fall bietet das Bundesrecht und Landesrecht (Hanebuth, 2011):

- Sicherheitssoftware KBA
- Netzgesetz des Bundes
- Vermittlungsstelle in Schleswig-Holstein im Meldegesetz zur Kommunikation der Meldebehörden bei der elektronischen Rückmeldung

Zu (2): Aufträge, deren Auftragswerte bestimmte Schwellenwerte erreichen oder überschreiten, sind gemäß § 100 Abs. 1 GWB vom Vergaberecht befreit. Diese Schwellenwerte werden durch Rechtsverordnung nach § 127 GWB festgelegt. Europaweit sind es ca. über 206.000 € bei Vergabe- und Vertragsordnungen für Leistungen (VOL). In den Bundesländern der Bundesrepublik Deutschland gelten unterschiedliche Vergabeverordnungen (Hanebuth, 2011).

Zu (3): Eine erhöhte Sicherheit liegt bspw. bei der Gewährleistung von Instanthaltung und Betreibung von Justizvollzugsanstalten oder Ähnlichem vor.

Zu (4): Eine Inhouse-Voraussetzung ist nach dem Europäischen Gerichtshof (EuGH) (EuGH Az. C-573/07, 2009) eine gemeinsame Verwaltungseinrichtung mit gemeinsamer Trägerschaft, deren Beherrschung durch die Träger

- wie bei einer eigene Dienststelle funktioniert,
- die Geschäfte wesentlich mit öffentlichen Trägern erfolgen,
- keine privaten Beteiligungen existieren und
- Geschäfte mit Dritten unter 10 % liegen (Hanebuth, 2011).

Zu (5): Für die Inhouse-Voraussetzungen bedarf es der Gründung einer gemeinsamen Organisation. Um diese Voraussetzung zu umgehen, lässt der EuGH die vergaberechtsfreie Zusammenarbeit von Verwaltungen auch zu, wenn eine öffentliche Aufgabe vorliegt, es sich dabei um keinen reinen Beschaffungsvorgang handelt und die kooperative Zusammenarbeit als „Schicksalsgemeinschaft“ bezeichnet werden kann (Hanebuth, 2011). Die Beteiligung Privater ist dabei nicht erlaubt. Konkret äußern sich die Anforderungen in folgenden Punkten (Hanebuth, 2011):

- Langfristige IT-Kooperation
- Kein alleiniger Austausch von Ware gegen Geld
- Kooperative Zusammenarbeit muss fortgeführt werden

- Keine Gewinnerzielungsabsicht
- Keine Haftung und Gewährleistung wie bei Beschaffungsvorgängen

In der Praxis zeigen sich Inhouse-Beispiele als „Anstalten des öffentlichen Rechts (AöR)“ oder einem Zweckverband bspw. in der Rechtsform einer gemeinnützigen GmbH (gGmbH). Solche Gesellschaften werden als Öffentlich-Öffentliche-Partnerschaften (ÖÖP) bezeichnet. Erfolgt eine Beteiligung von Privaten, so müssen diese Gesellschaften, Öffentlich-Private-Partnerschaften (ÖPP), am Vergabeprozess teilnehmen.

Im GGC-Lab ist die Bildung der Community Cloud auf Basis der Inhouse-Regelung vergaberechtsfrei möglich. Die öffentlich-rechtlichen IT-Dienstleister bilden eine gemeinsame Organisation, die Geschäfte mit ebenfalls öffentlichen Stellen (Kommunen, Verwaltungen,…) vorsieht. Die Vergabe und Abwicklung von Verträgen zum Kunden bleiben bestehen wie bisher und die einzelnen IT-Dienstleister bleiben die Ansprechpartner. Intern wird die Erfüllung des Vertrages unsichtbar für den Kunden in der Community Cloud abgewickelt.

Zusammenarbeiten werden durch Staatsverträge der jeweiligen Bundesländer realisiert. Diese Verträge sollte folgende Punkte beinhalten (Dataport, 2009):

- Errichtung, Beitritt, Rechtsform, Name, Sitz, Dienstsiegel
- Stammkapital, Vermögensübergang, Haftung, Anstaltslast
- Aufgaben, Beteiligungen
- Organe, Aufgaben der Organe
- Beschäftigte
- Rechtsaufsicht
- Wirtschaftsführung
- Datenschutz, Sicherheitsüberprüfung
- Laufzeit, Kündigung
- Veröffentlichungen
- Inkrafttreten

2.3.2. Spezialgesetzliche Regelungen

Spezialgesetzliche bzw. branchenspezifische Vorgaben ergeben sich u.a. aus der Pflicht der Unternehmensleitung zur Risikovorsorge (§§ 91, 93 AktG, §§ 35, 43 GmbHG) sowie spezialgesetzlichen Einzelregelungen (§ 25a Abs. 2 KWG, § 33 Abs. 2 WpHG). Durch unterschiedliche Anwendungsfälle greifen andere gesetzliche Regelungen. Wird die Bearbeitung von Arbeitnehmerdaten in Auftrag

gegeben greift das Arbeitnehmerdatenschutzrecht. Es muss nach Vorhaben und Anwendungsbereich unterschieden und geprüft werden ob zu diesem Vorhaben spezielle gesetzliche Reglungen existieren, z.B.:

- Telekommunikationsgesetz nach §§ 95 ff. oder § 92 TKG (Telekommunikationsgesetz)
- Handelsrechtliche Buchführungspflicht nach § 238 Abs. 1 in Verbindung mit § 257 Abs. 3 Nr. 2 HGB (Handelsgesetzbuch)
- Geheimnisträger nach § 203 StGB (Strafgesetzbuch) (Personen, wie Ärzte, Anwälte, Steuerberater usw.)
- Finanzdienstleistungen nach § 25a KWG (Kreditwesengesetz)
- Sozialdaten nach §§ 67 ff. SGB X
- Justiz, Polizei und Meldewesen
- Abgaben- und Steuerrecht nach §§ 146 ff. AO (Abgabenordnung)

Der Einsatz von Cloud Computing im öffentlichen Bereich erfordert eine genaue Betrachtung aller möglichen Fälle und Szenarien für die Bearbeitung der Daten. Sowohl Auftraggeber als auch Auftragnehmer müssen sich bspw. folgende Fragen stellen:

- Welche Art von Daten?
- Wer ist berechtigt die Daten zu bearbeiten?
- Wer könnte sich Vorteile durch einen Erhalt der Daten verschaffen?

Auch im GGC-Lab ist die Betrachtung spezialgesetzlicher Regelungen relevant und abhängig von der jeweiligen angebotenen Fachanwendung. Die Auswahl der Fachanwendungen für eine Datenverarbeitung in der Community Cloud kann entsprechend eingeschränkt werden, um solche speziellen Regelungen zu umgehen. Anwendungen, deren Daten eine hohe Vertraulichkeit aufweisen, können in der Community Cloud vermieden werden. Dies bleibt jedoch eine Einzelfallentscheidung und obliegt dem Aufnahmeprozess von Fachanwendungen in die Community Cloud. Generell ist jedoch davon abzuraten Daten mit besonders hoher Vertraulichkeit in der Public Cloud zu verarbeiten (Hofer, 2010).

2.3.3. Kartellrecht

Neben den branchenspezifischen Regelungen ist bei einem größeren Zusammenschluss von Anbietern die kartellrechtliche Bewertung eine kritische Frage. Das Kartellrecht wird in Deutschland im Gesetz gegen Wettbewerbsbeschränkungen (GWB) geregelt und verbietet „Vereinbarungen zwischen Unternehmen,

Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken“ (§ 1 GWB). Es findet laut § 130 Abs. 1 Satz 1 GWB auch „Anwendung auf Unternehmen, die ganz oder teilweise im Eigentum der öffentlichen Hand stehen oder die von ihr verwaltet oder betrieben werden“. Je nach Größe der Partner in der Community könnte ein Gebilde geschaffen werden, das als Wirkung den Wettbewerb verfälscht oder beherrscht (§ 18 Abs. 1 GWB). Dies ist der Fall, wenn z.B. eine Gesamtheit aus drei oder weniger Unternehmen zusammen einen Marktanteil von 50 % erreichen sowie fünf oder weniger einen Marktanteil von zwei Dritteln erreichen (§ 18 Abs. 6 GWB). Wird innerhalb der Community ein bestehender Wettbewerb nachgewiesen, kann die Vermutung der Marktbeherrschung jedoch widerlegt werden (§ 18 Abs. 7 GWB).

Im Projekt GGC schließen sich unter anderem große öffentlich-rechtliche IT-Dienstleister zusammen, die gemeinsam ein potentielles Nachfragekartell bilden könnten, z.B. wenn ein Großteil der deutschen Kommunen bzgl. einer Anwendung von der Community Cloud beliefert wird. Allerdings wird die geplante Erlösverteilung innerhalb der Community auf Basis eines Anreizsystems umgesetzt und fördert dabei den internen Wettbewerb. Deshalb greift möglicherweise die Ausnahmeregelung des § 18 Abs. 7 GWB. Dieser Fall muss durch die betreuende Rechtsabteilung eingehend geprüft werden, um abschließend beurteilt zu werden.

3 Fazit

Die Untersuchung hat gezeigt, dass die Vielfalt rechtlicher Rahmenbedingungen noch groß ist für die Etablierung von Cloud-Diensten im Öffentlichen Sektor. Dennoch existieren diverse Bestrebungen diese zu verstehen und sie positiv zu nutzen. Die wichtigsten rechtlichen Rahmenbedingungen für den Öffentlichen Sektor wurden im vorherigen Abschnitt angeschnitten. Für detailliertere und ausführende Informationen dienen diverse Leitfäden und Checklisten von verschiedenen Stellen und Verbänden. Um einen Überblick zu gewinnen werden deren Inhalte abschließend kurz vorgestellt (siehe Tabelle 2):

Tabelle 2: Überblick von Leitfäden bzgl. rechtlicher Rahmenbedingungen im Cloud Computing

Dokumententitel	Inhalte	Quelle
Leitfaden Cloud Computing – Recht, Datenschutz und Compliance	• Rechtliche Anforderungen zur Anbieterauswahl • Checkliste für Vertragselemente • Glossar	(Eckhardt, et al., 2010)
Rechtliche Anforderungen an Cloud Computing – Sichere Cloud-Dienste	• Rechtliche Anforderungen (Zivil-, Datenschutz-, Patent-/ Urheberrecht, Branchenspezifische Anforderungen) • Thesen zum rechtspolitischen Handlungsbedarf	(Duisberg, et al., 2011)
Orientierungshilfe – Cloud Computing	• Datenschutzrechtliche Aspekte • Technische und organisatorische Aspekte	(Budszus, et al., 2011)
Ein modernes Datenschutzrecht für das 21. Jahrhundert – Eckpunkte	• Datenschutzrecht	(BfDI, 2010)
Cloud Computing – Was Entscheider wissen müssen	• Positionierung, Vertragsrecht, Datenschutz • Informationssicherheit, Compliance	(BITKOM, 2010)
Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter	• Informationssicherheit • Vertragsgestaltung • Datenschutz und Compliance • Anforderungsvergleich in den verschiedenen Bereitstellungsmodellen	(BSI, 2010)
Cloud Computing in der öffentlichen Verwaltung	• Rahmenbedingungen • Risiken • Migrationsempfehlungen	(Fraunhofer FOKUS, 2010)
IT-Kooperationen	• Lösungsoptionen und Rahmenbedingungen für IT-Kooperationen im öffentlichen Sektor	(Graudenz & Schramm, 2010)
Empfehlungen für den Cloud Computing-Standort Deutschland	• Rechtsrahmen • Cloud in der öffentlichen Verwaltung • Ökosystem-Politik	(BITKOM & VOICE, 2012)
Leitfaden Compliance - Rechtliche Anforderungen an ITK-Unternehmen	• Compliance, Datenschutz • Korruptionsprävention • Wettbewerbsrecht, Kartellrecht • Außenwirtschaft, Finanzen, Abgaben • Lizenzen	(BITKOM, 2012)

Literaturverzeichnis

Armbrust, M. et al., 2009. Above the Clouds: A Berkeley View of Cloud Computing. *EECS Department, University of California, Berkeley*, 10 02.

BfDI, 2010. Ein modernes Datenschutzrecht für das 21. Jahrhundert - Eckpunkte. *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, 18 03.

BGH, Az. XII ZR 120/04, 2006. Urteil zur Rechtsnatur der Softwareüberlassung im Rahmen eines ASP-Vertrages.. *Bundesgerichtshof*, 15 11.

BITKOM, 2009. Cloud Computing Leitfaden. *Publikationen des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V.*, 10.

BITKOM, 2010. Cloud Computing – Was Entscheider wissen müssen. *Publikationen des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V.* , 12.

BITKOM, 2012. Leitfaden Compliance - Rechtliche Anforderungen an ITK-Unternehmen. *Publikationen des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V.*.

BITKOM & VOICE, 2012. Empfehlungen für den Cloud Computing-Standort Deutschland. *Publikationen des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. und VOICE e.V.*, 01 03.

BSI, 2010. Eckpunktepapier - Sicherheitsempfehlungen für Cloud Computing Anbieter. *Publikationen des Bundesamtes für Sicherheit in der Informationstechnik*, 27 09.

Budszus, J. et al., 2011. Orientierungshilfe – Cloud Computing. *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, 26 09.

Dataport, 2009. Staatsvertrag. *Dataport*, 04 11.

Duisberg, A. et al., 2011. IT-Gipfel - Rechtliche Anforderungen an Cloud Computing. *Eurocloud Deutschland*, 15 01.

Eckhardt, J. et al., 2010. Leitfaden Cloud Computing - Recht, Datenschutz & Compliance. *Eurocloud Deutschland*, 02 12.

EG Richtlinie 95/46/EG, 1995. Datenschutzrichtlinie. *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*.

Eriksdotter, H., 2011. Rechtsleitfaden für Cloud Computing. *CIO.de*, 03 01.

EuGH Az. C-573/07, 2009. Zulässigkeit einer vergaberechtsfreien In-House Vergabe an eine kommunal getragene Aktiengesellschaft. *Europäischer Gerichtshof*, 10 11.

Feld, C., 2013. Neue EU-Verordnung für Datenschutz im Internet. *ARD Tagesschau*, 09 01.

Fraunhofer FOKUS, 2010. Cloud Computing für öffentliche Verwaltung - ISPRAT Studie. *Publikationen des Fraunhofer-Institut für Offene Kommunikationssysteme*, 11.

Graudenz, D. & Schramm, G., 2010. IT-Kooperationen, Teil 1: Kontext, Lösungsoptionen und Rahmenbedingungen. *ISPRAT Whitepaper*.

Hanebuth, S., 2011. Zusammenarbeit der Verwaltungen - Vereinbarkeit mit dem Vergaberecht. *Dataport*, 17 01.

Hofer, T., 2010. Cloud Computing - Herausforderungen und Rechtsfragen. *Ludwig-Maxinilians Universität München Rechtsinformatikzentrum*.

Symantec, 2011. Öffentlicher Sektor genießt weiterhin größtes Vertrauen beim Datenschutz. *Emnid-Umfrage*, 27 07.

Trusted Cloud, 2012. Lizenzierungsbedarf beim Cloud Computing. *Arbeitspapier der AG Rechtsrahmen des Cloud Computing*, 11.

Volkmer, C., 2008. Datenschutz als Wettbewerbsvorteil?. *AIT feature,* Issue 2. Quartal, pp. 1-3.

Weichert, T., 2011. Cloud Computing und Datenschutz. *Datenschutzzentrum*, 14 11.

Bisher erschienene Bände der Schriftenreihe

Projektberichte IKM

ISSN 2196-3606 (online)

Band 01

Labes, Stine

Grundlagen des Cloud Computing.
Konzept und Bewertung von Cloud Computing

ISBN (online) 978-3-7983-2478-7
Published online 2012

Band 02

Erek, Koray; Drenkelfort, Gregor; Pröhl, Thorsten

Energiemonitoring von IKT-Systemen.
State-of-the-Art von Energiemonitoringsystemen

ISBN (online) 978-3-7983-2459-6
Published online 2013

Band 03

Drenkelfort, Gregor; Pröhl, Thorsten; Erek, Koray

Energiemonitoring von IKT-Systemen.
Kennzahlen

ISBN (online) 978-3-7983-2519-7
Published online 2013

Band 04

Drenkelfort, Gregor; Pröhl, Thorsten; Erek, Koray

Energiemonitoring von IKT-Systemen.
Periphere Energiebedarfe

ISBN (online) 978-3-7983-2520-3
Published online 2013

Band 05

Erek, Koray; Löser, Fabian; Grimm, Daniel

IKT-Performance Measurement Systeme.
State-of-the-Art

ISBN (online) 978-3-7983-2521-0
Published online 2013

Band 06

Erek, Koray; Opitz, Nicky; Pröhl, Thorsten

Geschäftsprozessmodellierung.
Kriterien und Methoden der Prozessmodellierung für ein Management-Cockpit

ISBN (online) 978-3-7983-2522-7
Published online 2013

Band 07

Opitz, Nicky; Pröhl, Thorsten; Erek, Koray

Cloud-Computing.
Kriterien und Umsetzung der Ressourcenmodellierung für ein Management-Cockpit

ISBN (online) 978-3-7983-2522-7
Published online 2013

Band 08

Labes, Stine

Grundlagen des Cloud Computing.
Cloud Computing in der Öffentlichen Verwaltung

ISBN (online) 978-3-7983-2612-5
Published online 2013

Band 09

Labes, Stine

Grundlagen des Cloud Computing.
Anforderungen an einen Cloud-Dienst

ISBN (online) 978-3-7983-2613-2
Published online 2013

Die rechtliche Situation und limitierende Rahmenbedingungen sind heute die größte Hürde für die Akzeptanz neuartiger Datenverarbeitung, wie im Cloud Computing. Besonders im Öffentlichen Sektor findet schon heute Datenverkehr und Kommunikation übergreifend über Einrichtungen sowie Städte- und Landesgrenzen hinweg statt. Ob dies künftig auch über Cloud-Dienste abgewickelt werden kann wird in diesem Dokument untersucht.

Mit Fokus auf die Situation im Projekt GGC-Lab, fasst der vorliegende Leitfaden die rechtlichen Themengebiete Vertragsgestaltung sowie Datenschutz und Compliance im Rahmen von Cloud-Diensten zusammen und zeigt Hindernisse auf. Die vertragliche Einordnung von Cloud-Diensten bewirkt unterschiedliche Anforderungen an die Verfügbarkeit des Dienstes sowie Gewährleistung und Haftung bei Verstößen. Für einen Zusammenschluss von öffentlich-rechtlichen IT-Dienstleistern, wie im Projekt GGC-Lab, gelten besondere Bedingungen hinsichtlich des Vergaberechts. Mit Hilfe eines Community-Vertrags werden alle internen Vereinbarungen, Qualitätslevel und Haftungsfragen geklärt. Mit dem Ziel der gemeinsamen Datenverarbeitung von cloudfähigen Fachanwendungen, müssen darüber hinaus spezielle Lizenzverträge mit dem Anbieter der jeweiligen Fachanwendung vereinbart werden. Bei der Verarbeitung personenbezogener Daten mit cloudbasierten Fachanwendung müssen die Forderungen des Datenschutzrechts beachtet werden. Werden durch den Zusammenschluss der IT-Dienstleister wettbewerbsbeeinflussend viele Abnehmer angesprochen, ist die Betrachtung des Kartellrechts eine weitere Hürde, die zu nehmen ist.

Viele Initiativen beschäftigen sich mit diesen komplexen Rechtsfragen und geben Vorschläge wie ihnen zu begegnen ist. Abschließend gibt eine Übersicht über die Inhalte ausführlicher Publikationen Aufschluss über den Stand der gegenwärtigen Diskussionen in diesem Themengebiet.

Universitätsverlag der TU Berlin

ISBN 978-3-7983-2627-9 (online)